AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Facebook, Inc. account located at www.Facebook.com/Markis.Jordan.7, as detailed in Attachment A

Case No. 4:17SW31

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to Commit Bank Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

See affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:
Kaitlin C. Gratton
Kaitlin C. Gratton
Assistant United States Attorney

Applicant's signature

Derek M. Mullins, United States Postal Inspector
Printed name and title

Sworn to before me and signed in my presence.

Date: June 9, 2017

Judge's signature

City and state: Norfolk, Virginia

The Honorable Robert J. Krask, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

IN RE SEARCH OF	)	~~UNDER SEAL~~
	)	
INFORMATION ASSOCIATED	)	
WITH FACEBOOK, INC. ACCOUNT	)	
	)	
1) www.Facebook.Com/**Markis.Jordan.7**	)	~~4:17-mj~~ 4:17SW31
	)	
THAT IS STORED AT	)	
PREMISES CONTROLLED BY	)	
FACEBOOK, INC.	)	

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek Mullins, being duly sworn, hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit in support of an application for a search warrant for information associated with a certain Facebook account that is stored at premises owned, maintained, controlled, or operated by a social-networking company owned by Facebook, Inc. ("Facebook") and headquartered in Menlo Park, California, as described in Attachment A. The information to be searched is described in the following paragraphs and in Attachment B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the accounts described in Attachment A, including the contents of communications. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS"). I have been employed as a Postal Inspector since April 2015. Prior to becoming a Postal Inspector I was employed by the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") since August 2008. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigators Training Program and the U.S. Immigration and Customs Enforcement Academy's ICE Special Agent Training Program. Prior to my employment with HSI, I was a Deputy Sheriff with the Wise County Sheriff's Department in Wise County, Virginia from 2005 to 2008. I have received training in various aspects of federal law enforcement including the investigation of identity theft, fraud, and narcotics related offenses as well as numerous other federal and state offenses. I have participated in multiple investigations, seizures, and search warrants, which have resulted in criminal arrests, seizures, and prosecutions. I have also been the affiant on search, arrest, and seizure warrants that have resulted in successful arrests, seizures and prosecutions.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (Conspiracy to Commit Bank Fraud), 1344 (Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft) have been committed by Markis Dickerson ("DICKERSON"), Christopher BOONE ("BOONE"), and other

RJK

DHW

persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes and items to be seized listed in Attachment B.

RELEVANT STATUTES

5. Title 18, United States Code, Sections 1349 prohibits any person from "attempt[ing] or conspir[ing] to commit any offense under this chapter." Sections 1344 is contained in the same chapter.

6. Title 18, United States Code, Sections 1344 prohibits anyone from "knowingly execut[ing], or attempt[ing] to execute, a scheme or artifice—(1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations or promises."

7. Title 18, United States Code, Section 1028A prohibits anyone, during and in relation to any enumerated felony violation, from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. Title 18, United States Code, Section 1028A enumerates felony violations, including any provision contained in chapter 63 (relating to mail, bank, and wire fraud).

PROBABLE CAUSE

8. In December 2014, I became involved in an investigation into a group of individuals who were using financial institutions to negotiate fraudulent assets into cash withdrawals from ATMs. The fraud scheme began in or about August 2014 and involved the suspects soliciting current bank accountholders on social media sites, including Facebook and Instagram. At the suspects' direction and in exchange for promise of payment, the accountholders would provide their debit/credit cards and PIN numbers. The suspects would

RJK

DMM

then deposit worthless or stolen checks into the compromised accounts using various ATMs in the Hampton Roads area of Virginia. Once the checks were deposited at an ATM, the bank of deposit credited the account of deposit with all or some of the check's stated value. The suspects would then make ATM withdrawals and conduct other transactions to access the maximum allowable amount each day the account was used in the scheme. When the suspects were conducting the fraudulent withdrawals or deposits, the financial institutions had cameras recording the transactions.

9. During this investigation, Markis Jordan DICKERSON ("DICKERSON") was identified, through interviews of accountholders and debriefs of defendants, as one of the individuals conducting this scheme, alone and with others, throughout the Hampton Roads area of Virginia.

10. As part of this investigation, investigators were able to view some of DICKERSON'S publicly available activity on Facebook and Instagram. Investigators saw numerous photographs of DICKERSON holding large quantities of cash, debit/credit cards, firearms, narcotics, and ATM receipts. Investigators also identified conversations on DICKERSON'S social media accounts in which DICKERSON was soliciting accountholders for their debit/credit cards to engage in the fraud scheme. For example, investigators identified a January 2015 Facebook conversation between DICKERSON and C.W. in which DICKERSON messaged C.W. and stated, "If you got a bank account and you trynna make a couple thousand let me know." During this conversation, DICKERSON explained to C.W. how to set up a bank account and provide the "bank card" and "4 digit PIN." DICKERSON further explained that he has been able to take "official bank business checks" and "deposit 5 racks in one account."

11. In addition to these conversations, on January 22, 2015, a state search warrant was executed on an iPhone 5C bearing serial number: C7KLLA31FFHH belonging to DICKERSON. During the search of the phone, investigators located numerous photographs depicting bank receipts; debit cards; and DICKERSON posing with large sums of U.S. currency, firearms, and narcotics. Specifically, one photograph depicted two Bayport Credit Union receipts dated December 11, 2014. Both receipts showed the last four digits of the account number. One of the receipts showed a balance of $5514.51 and the second showed a balance of $5625. Five photographs of debit cards bearing names other than DICKERSON's were identified. There was also an "account snapshot" of a Langley Federal Credit Union ("LFCU") account issued to an individual named E.B. The snapshot depicts a balance of $6,089 on December 18, 2014 and returned deposit check for -$6,084 on December 30, 2014. There was also a photograph of DICKERSON standing with a stack of U.S. currency against his ear, as if he were talking on a telephone, and holding a black handgun with an extended magazine in the other hand.

12. As a result of the 2014 investigation, four individuals were charged and convicted in the Eastern District of Virginia of conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1). *United States v. Frazier et al.*, 4:15cr43. DICKERSON was not charged in the original investigation.

13. In approximately December 2016, I was contacted by an LFCU fraud investigator requesting assistance with an investigation that involves DICKERSON, Christopher Douglas BOONE ("BOONE"), and others concerning the use of LFCU and other financial institutions to negotiate worthless and counterfeit financial instruments into U.S. currency and other instruments. The investigator indicated that LFCU had discovered numerous transactions in multiple LFCU accounts involving the deposit of fraudulent checks and money orders and

RJK

DHL

subsequent withdrawal and use of the funds credited on such deposits. LFCU had also identified purchases of money orders from retail locations through which DICKERSON, BOONE, and others obtained the cash value of the fraudulently deposited instruments. LFCU had identified and preserved video and still surveillance images of DICKERSON, BOONE, and others conducting the transactions.

14. LFCU is a federally insured financial institution, as defined in 18 U.S.C. § 20.

15. The LFCU investigator was able to identify and interview numerous accountholders whose accounts had been used to effect the fraudulent transactions. According to the LFCU investigator, many accountholders reported that DICKERSON and others had contacted them via social media outlets to solicit their banking information. Specifically, DICKERSON and others first posted a public message seeking accountholders interested in making money. DICKERSON and others would then send private or direct messages to those who responded positively to the public message. In these private and direct messages, DICKERSON and others generally requested that all further communications be conducted via text messages or telephone calls. DICKERSON and others then directed accountholders to provide their debit cards and PINs to DICKERSON, BOONE, and others. DICKERSON and others arranged to meet accountholders at various locations to obtain debit cards and PINs, promising to deposit money into the accounts associated with such debit cards. DICKERSON, BOONE, and others then used those debit cards and PINs to effect deposits of worthless and counterfeit financial instruments, including checks and money orders, into the associated accounts. Once funds were credited to those accounts, DICKERSON, BOONE, and others used the associated debit cards and PINs to withdraw U.S. currency from ATMs and to make purchases at retail locations.

RJK

DMA

16. Debit card numbers and PINs are means of identification, as defined in 18 U.S.C. § 1028(d)(7), for the accountholders to which they are assigned.

17. Through the investigation, as described further herein, your affiant has learned that the Facebook account of Markis DICKERSON is an account that is provided through Facebook. Through internet open source search on Facebook for DICKERSON it was found that he had his own Facebook account. While viewing the "open" portion of DICKERSON's Facebook account and by viewing several of the accountholders' Facebook accounts, investigators were able to link DICKERSON as Facebook "friends" with several of the solicited bank accountholders. Based on information gathered during the course of this investigation, I have identified one Facebook account that DICKERSON has used to solicit and communicate with accountholders and others in furtherance of the scheme. This is the account located at www.Facebook.Com/Markis.Jordan.7.

18. As part of this investigation, I have reviewed additional postings and messages made to and through Instagram and Facebook accounts in which DICKERSON and others have discussed and attempted to further the scheme. The following are examples of such postings:

a. During the execution of a state search warrant on a Facebook account belonging to D.G., an associate of DICKERSON, investigators identified an October 31, 2016 series of direct messages between D.G. and DICKERSON concerning the scheme. DICKERSON was using the Facebook account located at http://www.facebook.com/markis.jordan.7, which was then listed under the username "Freeband Jordan." That account is currently listed under the username "Lee Swervo."

In the October 31, 2016 conversation, D.G. asked DICKERSON to explain "dat money train." DICKERSON responded, "Gotta find people wit bank accounts." D.G. stated that "presto" had been telling him/her to "get on that shit the other day navy and langly." DICKERSON responded, "Yea shit crazy we was all gettin money out here before him and Ki Ki got locked but they was droppin fake checks and sometimes it would clear but I ran into da plug himself he make the official shit on his laptop and everything it ain't no where near how we used to do it."

As a result of the 2014 investigation, I know that "presto" is a nickname used by Preston Frazier and "Ki Ki" is a nickname used by Keandre Williams. Both of these individuals were prosecuted and convicted in that investigation. *See United States v. Frazier et al.*, 4:15cr43.

b. In December 2016, investigators were monitoring DICKERSON's public Instagram account, then associated with the username "freebandkid23." Investigators observed an image posted to that account depicting an LFCU account overview, as it would appear when the account is accessed through an online banking application. The overview includes the Smart Checking and Savings accounts belonging to H.B., an accountholder investigators have associated with the current scheme. This screenshot was posted along with the following message: "Who got Langley and want 3800 in their account by tomorrow morning??"

c. In February 2017, investigators were again monitoring DICKERSON's public Instagram account. At that time, the account was associated with the user name "freebandswervo." The account appeared be the same account previously associated with the username "freebandkid23."[1] Investigators observed an image posted to that account depicting a USAA account overview, as it would appear when the account is accessed through an online banking application. The overview includes a Classic Checking account belonging to H.F., another accountholder investigators have associated with the current scheme. The balance of the account was then $4,643.65. This screenshot was posted along with the following message: "Had me a good ol morning . . . HIT ME UP IF YOU WANT SOME MONEY IN YOUR ACCOUNT TODAY!!" In the days that followed this posting, investigators observed additional postings of screenshots depicting the same account with a higher available balance. One such posting showed a current balance of $12,759.24 and included the following messages: "Who want at least 4,000 in their account?" and "If you want at least 4,000 in your account DM me."

d. Also in February 2017, investigators observed an image posted to DICKERSON's public Instagram account, also made when the account was associated with the username "freebandswervo." That image depicted the same LFCU account overview for the account belonging to H.B., which investigators had previously observed in December 2016. This screenshot was re-posted along with the following message: "If you have Langley and want 3800 in your account DM me ASAP." Several Instagram users responded to the public post. DICKERSON replied on three occasions to these users advising them to contact him on his posted telephone number.

[1] Investigators have also associated the username "bigmoney_jordan" with that same account.

RJK

DMG

19. As part of this investigation, I have reviewed police reports filed by accountholders concerning their contact with DICKERSON and others. The following are examples of such reports:

a. According to a Newport News Police report, on or about January 6, 2017, DICKERSON contacted K.S. via social media and requested to use his/her bank account, purportedly because he was not able to access his own account. K.S. advised he/she "thought he was going to pay" him/her to use his/her bank account. They met and DICKERSON provided K.S. with two personal checks from his old account and requested he/she deposit them into his/her account. K.S. also gave DICKERSON his/her debit card and PIN. K.S. deposited the checks as requested and notified DICKERSON. K.S. was later contacted by his/her bank indicating that the checks he/she had deposited were fraudulent. K.S.'s bank further advised that additional counterfeit checks had been deposited into the account and cash withdrawals had been made at various ATMs, causing the account to be overdrawn. The bank also notified K.S. that a large purchase was made at Walmart. On January 30, 2017, Detective E. Benson met with the Asset Protection Manger at Walmart and viewed the surveillance video of the transaction described above. Detective E. Benson positively identified DICKERSON as the individual making the transaction.

b. According to a Hampton Police report, on or about January 17, 2017, DICKERSON contacted E.L. via social media and indicated that he could "make [him/her] some money." According to the police report, DICKERSON deposited four counterfeit checks into E.L.'s account totaling $3,853.43. After the money was deposited, DICKERSON contacted E.L. to obtain the online username and password for his/her LFCU account. DICKERSON advised he needed to login to the account and see if the money was available. DICKERSON also stated he needed to physically obtain E.L.'s debit card and PIN to ensure E.L. would "not go to the bank and steal all the money." On January 17, 2017, DICKERSON drove to E.L.'s residence and retrieved his/her debit card and PIN. On January 18, 2017, E.L. contacted LFCU and discovered that $500 had been withdrawn from the account via ATM. E.L. stated there were no funds in his/her account prior to DICKERSON depositing the counterfeit checks.

20. From approximately at least December 2016 through April 13, 2017, DICKERSON, BOONE, and others have participated in ATM transactions on more than 45 accounts issued by LFCU, SunTrust Bank ("SunTrust"), 1st Advantage Federal Credit Union ("1st Advantage"), and other financial institutions, all of which are federally insured financial

RJK

DMM

institutions, as defined in 18 U.S.C. § 20. In each of these transactions, U.S. currency was withdrawn following the deposit of a worthless or counterfeit financial instrument via "remote capture deposit." A "remote capture deposit" is a deposit accomplished through the transmission of information to the institution of deposit via a mobile application on an electronic device with either cellular or internet access. During each of the withdrawals that followed such deposits, DICKERSON and BOONE were captured by ATM surveillance equipment either personally conducting the transaction or accompanying the individual(s) who conducted the transaction. Through review of LFCU's records and its interviews with actual accountholders, investigators have determined that during the period of time surrounding these transactions, the individual through whose account the transaction was done had telephonic contact with DICKERSON and/or BOONE.

21. The following are examples of the transactions identified to date as being associated with DICKERSON and BOONE:

a. On December 13, 2016, three fraudulent checks were deposited into K.M.'s LFCU account via remote capture deposit. On the same day, four transactions were attempted/conducted at an LFCU branch located on West Mercury Boulevard in Hampton, Virginia. The first transaction was an attempted ATM withdrawal at the drive-thru ATM using K.M.'s debit card and PIN. BOONE was captured by the ATM's surveillance equipment driving a black car through the drive-thru ATM and attempting to withdraw $500 from K.M's account at that ATM. After the transaction was declined, BOONE then attempted a second successful withdraw of $300 from K.M.'s account. DICKERSON was captured by the ATM's surveillance equipment in the passenger seat beside BOONE during these transactions. Approximately two minutes after BOONE drove away from the ATM, DICKERSON was captured by the walk-up ATM's surveillance equipment conducting two separate withdrawals; each for $100. K.M.'s debit card and PIN were used during each of these transactions.

b. On January 26, 2017, three counterfeit checks were deposited into J.B.'s LFCU account via remote capture deposit. That same day, BOONE was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw $500 from J.B.'s account at the drive-thru LFCU ATM located on

RJK

DMG

West Mercury Boulevard in Hampton, Virginia. On January 29, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. On January 30, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw $500 from J.B.'s account at the walk-up ATM at the same LFCU branch located on West Mercury Boulevard in Hampton, Virginia.

22. On March 1, 2017, DICKERSON and BOONE were arrested by the Newport News Police Department, Hampton Police Division, and the United States Postal Inspection Service during a traffic stop in Hampton, Virginia. On that date, DICKERSON was observed driving a 2009 Mercedes Benz, white in color, registered to DICKERSON through the Virginia Department of Motor Vehicles, with two other occupants. BOONE was identified as the sole rear-seat passenger, located immediately behind the driver. At the time of his arrest, DICKERSON was found with a stolen handgun loaded with a high-capacity magazine concealed in his waist band. Incident to arrest, the vehicle was searched for weapons immediately accessible to DICKERSON or the other passengers in the vehicle. A second handgun was found under the driver's seat, immediately accessible to BOONE. Inspection of the driver's seat revealed that the area from which this second handgun was recovered was not accessible from the driver's seat, only from the rear passenger seat, as a result of the motorized seat components. During the weapons sweep of the vehicle, investigators also observed credit/debit cards bearing names of individuals who were not in the vehicle. At that time, investigators stopped the search, maintained control of the vehicle, and applied for a state search warrant.

23. That same day, investigators executed a state issued search warrant on the vehicle described above. During the search, investigators located more credit/debit cards bearing names of individuals who were not in the vehicle; two counterfeit checks bearing the City of Norfolk seal and the name of a known accountholder; an HP laptop computer, model number 2000-

410US; a printer; and numerous pages of blank check stock. Investigators also seized three cellular telephones: a black iPhone, Model A1778; and a pink iPhone, Model A1687; and a silver iPhone, Model A1549. The black and pink iPhones belonged to BOONE and the silver iPhone belonged to DICKERSON.

24. Based on information gathered from the investigation, investigators applied for and were issued a state search warrant for BOONE's residence located on Friendly Drive, in Hampton, Virginia. Investigators executed the search warrant on BOONE's residence on March 1, 2017. Inside the residence, investigators located and seized, among other items, two printers, an HP laptop computer, model Notebook 15-F233WM, hundreds of pages of blank check stock, numerous credit/debit cards in various names, counterfeit checks bearing the City of Norfolk seal and the name of the same known accountholder printed on the counterfeit checks found in DICKERSON's vehicle.

25. All of the items that were seized during the execution of the warrants on March 1, 2017 were packaged and placed into evidence at the Hampton Police Department. On April 27, 2017, these items were transferred to the United States Postal Inspection Service and placed into evidence, where they remain.

26. Based on the information obtained from the investigation and evidence recovered during the execution of the above-described warrants, BOONE and DICKERSON were both charged in Hampton, Virginia with 18.2-178 (Obtaining Money by False Pretense). BOONE was also charged with 18.2-308.2 (Possession of a Firearm by a Convicted Felon).

27. BOONE remained in stated custody after after his arrest on March 1, 2017.

RJK

DRM

28. On March 9, 2017, DICKERSON was issued a bond in the Hampton, Virginia Court. DICKERSON posted bond later the same evening and was released from the Hampton, Virginia jail.

29. After his release, DICKERSON was identified in ATM surveillance images conducting additional transactions to access funds credited to accounts following remote capture deposits of worthless and counterfeit checks, including but not limited to the following transactions:

a. On April 5, 2017, a counterfeit check was deposited into A.O.'s LFCU account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using A.O.'s debit card and PIN attempting to withdraw $500 from A.O.'s account at a walk-up ATM located on Jefferson Avenue in Newport News, Virginia.

b. On April 12, 2017, DICKERSON was captured by ATM surveillance equipment depositing an altered Western Union money order into D.G.'s 1st Advantage Bank account. That same day, DICKERSON was again captured by ATM surveillance equipment using D.G.'s debit card and PIN as he withdrew $100 from D.G.'s account at the drive-through ATM located at the 1st Advantage Bank on West Mercury Boulevard in Hampton, Virginia.

30. On April 12, 2017, a federal grand jury sitting in Newport News returned a 17-count indictment charging DICKERSON and BOONE with conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349 (Count 1); bank fraud, in violation of 18 U.S.C. § 1344 (Counts 2-9); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Counts 10-16). The indictment also charged BOONE with possessing a firearm as a convicted felon, in violation of 18 U.S.C. § 922(g)(1) (Count 17).

31. On April 13, 2017, DICKERSON was pulled over in a traffic stop in Hampton, Virginia. On that occasion, DICKERSON was driving the same vehicle he had been operating on March 1, 2017. During the stop, DICKERSON was arrested on the outstanding federal arrest

RJK

DMR

warrant. Incident to arrest, officers from the Hampton Police Division located on DICKERSON's person a black and silver Alcatel One Touch cellular telephone. After arresting DICKERSON, officers conducted an inventory of DICKERSON's 2009 Mercedes Benz prior to having it towed. During the inventory, officers located several debit cards within the passenger compartment, immediately accessible to the driver's seat. Two of the debit cards were in the names A.O. and D.G., accountholders whose accounts DICKERSON accessed after he was released on bond, as described above. Officers also located in the passenger compartment a white Samsung Galaxy Grand Prime cellular telephone, as well as a printer and blank check stock.

32. All of the items that were recovered from the inventory of DICKERSON's vehicle were turned over to Newport News Police Detective and U.S. Postal Inspection Service Task Force Officer (TFO) E. Benson. These items were entered into to Newport News Property and Evidence, where they currently remain.

33. DICKERSON made his initial appearance on April 14, 2017. Boone made his initial appearance on June 2, 2017. Trial is currently set for September 6, 2017.

LEGAL AUTHORITY

34. The legal authority for this search warrant application regarding the Facebook account is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic

RJK

communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

35. 18 U.S.C. § 2703(b) provides in relevant part as follows:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> (A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.
>
> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
>
> (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

36. The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. Title 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

37. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated herein. On January 13, 2017, Newport News Police Detective Emily Benson sent a preservation

RJK

request to Facebook pursuant to 18 U.S.C. § 2703(f), requiring Facebook to maintain the contents of the aforementioned account.

DEFINITIONS

38. The term "computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

39. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

a. documents, spreadsheets, records or representations;

b. photographs;

c. pictures;

d. images, and

e. aural records or representations.

40. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

41. Universal Resource Locator (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL

RJK

DMM

of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

42. Internet Protocol Address (IP Address): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses; static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

43. Internet Service Providers (ISPs): Individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

44. A "MAC Address" refers to the fact that every computer has a unique identifying number that is placed there by the manufacturer. It is based on a set standard on which all manufactures have agreed, and no two MAC Addresses are alike. A MAC Address is similar to the VIN number of a vehicle, as the number is not changeable.

45. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a

server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

46. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

47. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

48. "Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

49. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

50. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of

RJC

DMA

such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

TECHNICAL BACKGROUND

51. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com.

52. Facebook allows its users to establish accounts with Facebook, and users can use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

53. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen numbers, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

54. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

RJK
DMA

55. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

56. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check-in" to particular location or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

57. Facebook allows users to upload photos and videos. It also provides users the ability to "tag" (*i.e.*, label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

RJK

58. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are store in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

59. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

60. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

61. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

62. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

63. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

64. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that h or she has been "poked" by the sender.

65. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

66. Facebook allows its users to share live videos through a feature called "Facebook Live." These videos are live-streamed in accordance with the users' privacy settings, through which the user designates who may view their postings, including other Facebook users and the public, in general. When the videos are streamed live, a red icon appears at the top left-hand corner of the video indicating that it is a live video. The word "Live" is written next to the icon, along with the number of current viewers. After the user ends a Facebook Live broadcast, the video is published to the user's page or profile, just like any other post, where it remains available for viewing until such time as the user removes it.

67. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user's access or use of that application may appear on the user's profile page.

RJK

DMM

68. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

69. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

70. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

RJK

DMM

71. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, which would include information such as the IP addresses and devices used to access the account; transaction information; and other account information that might be used to identify the actual user or users of the account at particular times.

SEARCH PROCEDURES

72. The search warrant will be sent electronically via the Facebook Law Enforcement Online Requests portal to personnel with Facebook who will be directed to produce the information noted in the warrant. Consistent with the procedures outlined in Attachment B, your affiant and other agents will review the production and seize those e-mails and/or records that are authorized by the search warrant.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

73. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the production and seize those items described in Section II of Attachment B.

CONCLUSION

74. Based on the facts set forth above, I submit that probable cause exists to believe the user of the Facebook account located at www.Facebook.Com/Markis.Jordan.7, believed to be

Markis Jordan Dickerson, has violated 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft), and that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within the information associated with the Facebook account.

75. Accordingly, I request that a warrant be issued authorizing the United States Postal Inspection Service, with assistance from other law enforcement personnel, to search those premises noted in Attachment A and obtain the information in the account for the items noted in Attachment B.

76. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

77. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Facebook, Inc. accepts out-of-state and out-of-district service of subpoenas, court orders, and search warrants via the Law Enforcement Online Requests portal without the presence of a law enforcement officer. Accordingly, your affiant will execute the requested search warrant by e-mail to the custodian of records at Facebook, Inc. and permission is requested for the data to be copied / obtained outside of the presence of a law enforcement officer. It is anticipated that Facebook, Inc. will produce the requested records in electronic format accompanied by a signed authentication letter via E-mail or on electronic media via U.S. Mail to your affiant.

Respectfully submitted,

Derek M. Mullins
United States Postal Inspection Service

This affidavit has been reviewed for legal sufficiency by:

Kaitlin C. Gratton

Kaitlin C. Gratton
Assistant United States Attorney

Subscribed and sworn to before me this 9th day of June, 2017, in the City of ~~Newport News~~ Norfolk, Virginia.

/s/ Robert J. Krask

UNITED STATES MAGISTRATE JUDGE

RJK

DMK

ATTACHMENT A

PROPERTY TO BE SEARCHED

This search warrant applies to information associated with the Facebook user ID:

(1) www.Facebook.Com/Markis.Jordan.7

that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

RJK

DMW

ATTACHMENT B

PARTICULAR ITEMS TO BE SEIZED

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including all Facebook Live videos and broadcasts;

(e) All profile information; News Feed information; status updates; links to videos; photographs; articles, and other items; Notes; Wall postings; friend lists; including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook identification numbers; future and past event postings; rejected "Friend" requests; comments;

RJK

DMA

gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(f) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(g) All IP logs, including all records of the IP addresses that logged into the account

(h) All past and present lists of friends created by the account;

(i) All information about the user's access and use of Facebook Marketplace;

(j) The types of service utilized by the user;

(k) All "check-ins" and other location information, including all geo-location information associated with the user's postings and messages;

(l) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(m) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. §1028A(a)(1) (Aggravated Identity Theft), those violations involving Markis DICKERSON and other co-conspirators occurring after **August 1,**

RJK

DMM

2014, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications and any account content and information involving and concerning the recruitment and solicitation of accountholders;

(b) Communications and any account content and information about or reflecting the recruitment process;

(c) Communications among known and unknown co-conspirators;

(d) Preparatory steps taken in furtherance of the fraud scheme;

(e) Records of association, including friend lists and friend requests among conspirators and accountholders, presently known and unknown;

(f) All profile information, account content and information, and communications relating to violations of 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. §1028A(a)(1) (Aggravated Identity Theft); and

(g) Records relating to who created, used, accessed, or communicated with the account, including any records about their identities and whereabouts.